

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Confirmation No. 9927
Filed: **APRIL 2, 2004**

In the Claims:

Claims 1-11 (Cancelled).

12. (Currently Amended) A method for generating output bytes corresponding to respective input bytes according to a one-to-one binary function representing a cryptographic algorithm, the method comprising:

decoding an input byte and generating at least one bit string that contains only one active bit;

using an array of logic gates for logically combining bits of the at least one bit string according to the one-to-one binary function and generating a 256-bit string without the use of a lookup table; and

encoding the 256-bit string for obtaining an output byte for the cryptographic algorithm.

13. (Previously Presented) A method according to Claim 12, wherein the decoding comprises subdividing the input byte into a left nibble and a right nibble, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, each 16-bit string containing only one active bit; and wherein logically combining the bits comprises logically combining the 16-bit strings according to the one-to-one binary function for generating the 256-bit string.

14. (Previously Presented) A method according to Claim 12, wherein the input byte is decoded in a corresponding auxiliary 256-bit string; and the 256-bit string is obtained by changing an order of the bits of the auxiliary 256-bit string according to the one-to-one binary function.

In re Patent Application of:
MACCHETTI ET AL.
Serial No. **10/816,791**
Confirmation No. **9927**
Filed: **APRIL 2, 2004**

15. (Previously Presented) A method according to Claim 12, wherein the one-to-one binary function represents a ByteSub operation of a Rijndael AES encryption/decryption algorithm.

16. (Currently Amended) A method according to Claim 13, wherein the array of logic gates comprises AND gates, with each bit of the 256-bit string being ~~is~~ obtained by ANDing among the bits of the 16-bit strings.

17. (Currently Amended) A method for implementing a cryptographic algorithm comprising:

decoding an input byte and generating at least one bit string that contains only one e active bit;

using an array of logic gates for logically combining bits of the at least one bit string according to the one-to-one binary function and generating a bit string without the use of a lookup table; and

encoding the bit string for obtaining an output byte for the cryptographic algorithm.

18. (Previously Presented) A method according to Claim 17, wherein the cryptographic algorithm comprises a Rijndael AES encryption/decryption algorithm.

19. (Previously Presented) A method according to Claim 18, wherein the one-to-one binary function represents a ByteSub operation in the Rijndael AES encryption/decryption algorithm.

20. (Previously Presented) A method according to Claim 17, wherein the decoding comprises subdividing the input byte into

In re Patent Application of:

MACCHETTI ET AL.

Serial No. **10/816,791**

Confirmation No. **9927**

Filed: **APRIL 2, 2004**

a left nibble and a right nibble, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, each 16-bit string containing only one active bit; and wherein logically combining the bits comprises logically combining the 16-bit strings according to the one-to-one binary function for generating the bit string.

21. (Previously Presented) A method according to Claim 17, wherein the input byte is decoded in a corresponding auxiliary bit string; and the bit string is obtained by changing an order of the bits of the auxiliary bit string according to the one-to-one binary function.

22. (Currently Amended) A method according to Claim 20, wherein the array of logic gates comprises AND gates, with each bit of the bit string being ~~is~~ obtained by ANDing among the bits of the 16-bit strings.

23. (Currently Amended) A device for implementing a cryptographic algorithm, the device comprising:

a decoder for decoding an input byte and generating at least one bit string that contains only one active bit;

an array of logic gates being input with the at least one bit string, and generating a 256-bit string without the use of a lookup table by logically combining the bits of the at least one bit string according to the one-to-one binary function; and

an encoder being input with the 256-bit string and generating an output byte for the cryptographic algorithm.

24. (Previously Presented) A device according to Claim

In re Patent Application of:

MACCHETTI ET AL.

Serial No. **10/816,791**

Confirmation No. **9927**

Filed: **APRIL 2, 2004**

23, wherein said decoder comprises a left decoder and a right decoder being input with a left nibble and a right nibble of the input byte, and generating a left 16-bit string and a right 16-bit string, respectively, each containing only one active bit; said array of logic gates generating the 256-bit string as a logic combination of bits of the 16-bit strings.

25. (Previously Presented) A device according to Claim 24, wherein said array of logic gates comprises an array of 256 AND gates, each AND gate generating a respective bit of the 256-bit string by ANDing bits of the 16-bit strings.

26. (Previously Presented) A device according to Claim 24, further comprising:

an array of multiplexers each being input with bits of the 16-bit strings and being driven by selection signals, and generating a respective intermediate bit being fed to said array of logic gates; and

said array of logic gates generating bits of the 256-bit string by logically combining the intermediate bits.

27. (Previously Presented) A device according to Claim 23, wherein said decoder generates a corresponding auxiliary 256-bit string; and said array of logic gates generates the 256-bit string by changing an order of the bits of the auxiliary 256-bit string according to the one-to-one binary function.

28. (Currently Amended) A cryptographic device for implementing a cryptographic algorithm, the cryptographic device comprising:

In re Patent Application of:

MACCHETTI ET AL.

Serial No. **10/816,791**

Confirmation No. **9927**

Filed: **APRIL 2, 2004**

a decoder for decoding an input byte and generating at least one bit string that contains only one active bit;

an array of logic gates being input with the at least one bit string, and generating a 256-bit string without the use of a lookup table by logically combining the bits of the at least one input string according to a one-to-one binary function; and

an encoder being input with the 256-bit string and generating an output byte for the cryptographic algorithm.

29. (Currently Amended) A cryptographic device according to Claim 28, wherein the cryptographic algorithm comprises ~~device implements~~ a Rijndael AES encryption/decryption algorithm.

30. (Previously Presented) A cryptographic device according to Claim 29, wherein the one-to-one function corresponds to a Bytesub operation within the Rijndael AES encryption/decryption algorithm.

31. (Previously Presented) A cryptographic device according to Claim 28, wherein said decoder comprises a left decoder and a right decoder being input with a left nibble and a right nibble of the input byte, and generating a left 16-bit string and a right 16-bit string, respectively, each containing only one active bit; said array of logic gates generating the 256-bit string as a logic combination of bits of the 16-bit strings.

32. (Previously Presented) A cryptographic device according to Claim 31, wherein said array of logic gates comprises an array of 256 AND gates, each AND gate generating a respective

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Confirmation No. 9927
Filed: **APRIL 2, 2004**

bit of the 256-bit string by ANDing bits of the 16-bit strings.

33. (Previously Presented) A cryptographic device according to Claim 31, further comprising:

an array of multiplexers each being input with bits of the 16-bit strings and being driven by selection signals, and generating a respective intermediate bit being fed to said array of logic gates; and

said array of logic gates generating bits of the 256-bit string by logically combining the intermediate bits.

34. (Previously Presented) A cryptographic device according to Claim 28, wherein said decoder generates a corresponding auxiliary 256-bit string; and said array of logic gates generates the 256-bit string by changing an order of the bits of the auxiliary 256-bit string according to the one-to-one binary function.